

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
8 March 2001 (08.03.2001)

PCT

(10) International Publication Number
WO 01/16900 A3

(51) International Patent Classification⁷: **G07F 7/10**,
G06F 1/00, G07F 7/08

(21) International Application Number: PCT/US00/23817

(22) International Filing Date: 30 August 2000 (30.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/151,880 31 August 1999 (31.08.1999) US
60/164,668 9 November 1999 (09.11.1999) US
60/165,577 15 November 1999 (15.11.1999) US
60/201,635 3 May 2000 (03.05.2000) US

(71) Applicant: **AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC.** [US/US];
American Express Tower, World Financial Center, New York City, NY 10285-4900 (US).

(72) Inventors: **BENNETT, Russell**; 10877 East Pear Tree Drive, Cornville, AZ 86325 (US). **BISHOP, Fred**; 2811

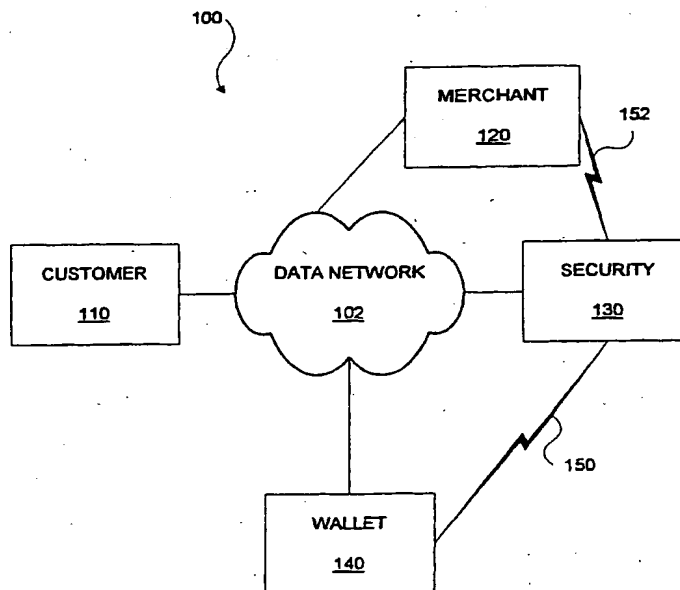
West Dynamite Boulevard, Phoenix, AZ 85085 (US). **GLAZER, Elliot**; 14107 Chiasso Terrace, Chesterfield, VA 23838 (US). **GORGOL, Zyg**; 10786 East Terra Drive, Scottsdale, AZ 85258 (US). **HOHLE, William, G.**; 10882 West Cedarfort Road (8570 North), Lehi, UT 84043 (US). **JOHNSTONE, David**; 28618 North 60th Place, Cave Creek, AZ 85331 (US). **LAKE, Walter, D.**; 719 West Rawhide Avenue, Gilbert, AZ 85233 (US). **SIMKIN, Marvin**; - (US). **SWIFT, Nick**; 38 Water Road, Reading, Greater London RG30 2NN (GB). **WHITE, Dirk**; 6638 West Via Montoya, Glendale, AZ 85310 (US). **JOHNSON, Michael**; 9154 North 97th Avenue, Peoria, AZ 85345 (US). **ROYER, Coby**; 7833 Stanford Avenue, University City, MO 63130 (US).

(74) Agent: **SOBELMAN, Howard, I.**; Snell & Wilmer L.L.P., One Arizona Center, 400 East Van Buren, Phoenix, AZ 85004-2202 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ,

[Continued on next page]

(54) Title: METHODS AND APPARATUS FOR CONDUCTING ELECTRONIC TRANSACTIONS



(57) Abstract: A system and method for conducting electronic commerce are disclosed. In various embodiments, the electronic transaction is a purchase transaction. A user (110) is provided with an intelligent token (202), such as a smartcard containing a digital certificate. The intelligent token suitably authenticates with a server on a network (130) that conducts all or portions of the transaction on behalf of the user. In various embodiments a wallet server (140) interacts with a security server (130) to provide enhanced reliability and confidence in the transaction. In various embodiments, the wallet server includes a toolbar (502). In various embodiments, the digital wallet pre-fills forms. Forms may be pre-filled using an auto-remember component.

WO 01/16900 A3



NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM,
TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

Published:

— with international search report

- (84) **Designated States (regional):** ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

- (88) **Date of publication of the international search report:**
4 October 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Intern. Application No
PCT/US 00/23817

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 G07F7/10 G06F1/00 G07F7/08		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 7 G07F G06F G06K H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 534 857 A (BOWCOCK MATTHEW P ET AL) 9 July 1996 (1996-07-09) abstract; figures 2,3 column 4, line 8 - line 25	1, 4, 13, 19, 22, 23
A	WO 99 21321 A (CRYPTOWORKS) 29 April 1999 (1999-04-29) abstract; figure 1 page 13, line 26 -page 15, line 28	1-3, 13, 15
P, A	EP 1 017 030 A (IBM) 5 July 2000 (2000-07-05) abstract; figures 4-6 page 7, line 35 -page 8, line 19 -/--	1-4, 13, 15, 22, 25, 30
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *Z* document member of the same patent family		
Date of the actual completion of the international search 19 April 2001		Date of mailing of the international search report 08. 05. 2001
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer Lindholm, A-M

INTERNATIONAL SEARCH REPORT

Intern. Application No.

PCT/US 00/23817

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 43 39 460 C (SIEMENS AG) 6 April 1995 (1995-04-06) abstract; figure 1 column 1, line 36 - line 53	1
X	US 5 832 212 A (CRAGUN BRIAN JOHN ET AL.) 3 November 1998 (1998-11-03) abstract column 2, line 14 - line 49 column 3, line 54 - column 4, line 50 column 5, line 66 - column 6, line 10	5-10
A	WO 98 21683 A (FINJAN SOFTWARE LTD) 22 May 1998 (1998-05-22) abstract page 3, line 4 - line 6 page 11, line 15 - line 22	5
A	WO 98 45778 A (ZUTA MARC) 15 October 1998 (1998-10-15) abstract page 17, line 4 - page 19, line 11	5
X	EP 0 917 120 A (CITICORP DEV CENTER INC) 19 May 1999 (1999-05-19) column 8, line 53 - column 10, line 9	25-31
X	EP 0 927 945 A (AMAZON COM INC) 7 July 1999 (1999-07-07) abstract column 2, line 14 - column 3, line 9	37-42

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 00/23817

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

As a result of the prior review under R. 40.2(e) PCT,
no additional fees are to be refunded.

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☒ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-4 13-24

Conducting transactions: After transaction request has been recieved at server. True identity of the smartcard owner is verified by challenge response (C+R). Credentials (session-, transaction-no.) comprising at least one key are assembled and provided to the user as well as a wallet server. Second request from user include part of credential. If this request is valid access to transaction is approved.

2. Claims: 5-12

Method to protect a network server by removing dangerous characters within the site an restricting access to portion of the server.

3. Claims: 25-41

Digital wallet comprising activator, toolbar as well as server.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. Application No

PCT/US 00/23817

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5534857 A	09-07-1996	AU 656245 B WO 9310509 A EP 0722596 A FI 942177 A NO 941774 A	27-01-1995 27-05-1993 24-07-1996 11-05-1994 11-05-1994
WO 9921321 A	29-04-1999	US 6026166 A AU 1105599 A EP 1033010 A	15-02-2000 10-05-1999 06-09-2000
EP 1017030 A	05-07-2000	JP 2000194770 A	14-07-2000
DE 4339460 C	06-04-1995	EP 0654919 A	24-05-1995
US 5832212 A	03-11-1998	CA 2251984 A EP 0894305 A WO 9740446 A	30-10-1997 03-02-1999 30-10-1997
WO 9821683 A	22-05-1998	EP 0965094 A US 6167520 A US 6092194 A US 6154844 A	22-12-1999 26-12-2000 18-07-2000 28-11-2000
WO 9845778 A	15-10-1998	AU 6850798 A	30-10-1998
EP 0917120 A	19-05-1999	AU 1584499 A AU 1796599 A AU 9234698 A BR 9806416 A CN 1233804 A EP 0917119 A EP 0950972 A JP 11250165 A JP 11232348 A TW 381241 B WO 9924891 A WO 9924892 A EP 0951158 A EP 0950992 A JP 2000036049 A JP 2000076189 A JP 2000251006 A	31-05-1999 31-05-1999 03-06-1999 16-11-1999 03-11-1999 19-05-1999 20-10-1999 17-09-1999 27-08-1999 01-02-2000 20-05-1999 20-05-1999 20-10-1999 20-10-1999 02-02-2000 14-03-2000 14-09-2000
EP 0927945 A	07-07-1999	US 5960411 A AU 9477998 A CA 2246933 A CA 2263781 A EP 0902381 A JP 11161717 A JP 2000099592 A WO 9913424 A	28-09-1999 29-03-1999 12-03-1999 12-03-1999 17-03-1999 18-06-1999 07-04-2000 18-03-1999



①9 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

⑫ **Offenlegungsschrift**
⑩ **DE 197 24 901 A 1**

⑤1 Int. Cl.⁶:
H 04 Q 7/32
H 04 Q 7/38
H 04 L 12/16

②1 Aktenzeichen: 197 24 901.9
②2 Anmeldetag: 12. 6. 97
④3 Offenlegungstag: 17. 12. 98

DE 197 24 901 A 1

⑦1 Anmelder:
Siemens Nixdorf Informationssysteme AG, 33106
Paderborn, DE

⑦4 Vertreter:
Epping, W., Dipl.-Ing. Dr.-Ing., Pat.-Anw., 82131
Gauting

⑦2 Erfinder:
Wiehler, Gerhard, 82223 Eichenau, DE

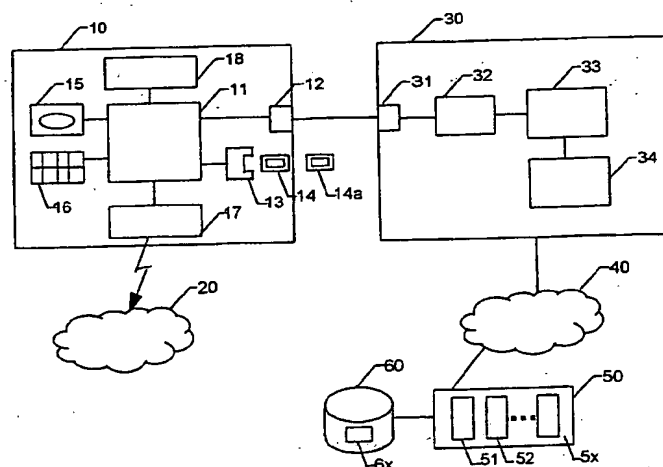
⑤6 Entgegenhaltungen:
DE 1 95 38 842 A1
DE 2 95 20 925 U1
DE 94 15 302 U1
GB 22 74 960 A
US 44 55 226
WO 95 15 065 A

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

⑤4 Mobilfunktelefon sowie solche mit gekoppeltem Rechner für Internet- bzw. Netzanwendungen und Verfahren zum Betreiben einer solchen Gerätekombination

⑤7 Anschluß der Kontakteinheit 13 des Mobilfunktelefons 10 über eine Steuereinheit 11 an die Anschlußschnittstelle 12 für den Rechner 30, so daß Daten zwischen einer Chipkarte 14/14a und der Anschlußschnittstelle 12 über die Steuereinheit austauschbar sind. Bei Kopplung mit einem Rechner 30 ist das Mobilfunktelefon 10 als Kartenterminal betreibbar, so daß vom Rechner 30 aus über ein Kommunikationsnetz 40 eine Inanspruchnahme der Netzdienste von Diensteanbietern 50 möglich ist. Chipkartenanwendungen z. B. für die gegenseitige Client-Server-Authentisierung, für die Verifikation von Zugriffsrechten, für die digitale Signatur sensibler Daten, für die Erzeugung von Schlüsseln zur Verschlüsselung von Daten, für den Beweis eines Bestellvorganges, für die Bezahlung aus einer elektronischen Börse usw.



DE 197 24 901 A 1

Die Erfindung betrifft Anordnungen und Verfahren für die Nutzung von im Internet oder in anderen Netzen angebotenen Leistungen, die hohe Sicherheitsanforderungen stellen.

Mobilfunktelefone werden im wesentlichen für die Sprachübertragung in Mobilfunknetzen benutzt. Das im Mobilfunktelefon integrierte sogenannte SIM-Modul bzw. die integrierte Chipkarte dient zur Authentisierung des Mobilfunktelefons als ein für den Mobilfunk berechtigtes Gerät und enthält Schlüssel für die Verschlüsselung der ausgesandten Sprachinformation bzw. für die Entschlüsselung der empfangenen Sprachinformation.

Rechner, wie z. B. Personalcomputer oder Laptops, die einen Festnetz- oder Mobilnetzanschluß aufweisen, sind in der Lage, z. B. mittels http-Protokoll, Internetanwendungen zu nutzen. Bei besonders sicherheitsrelevanten Vorgängen, wie z. B. bei Bestellungen und Zahlungen, werden Chipkarten verwendet, die über einen am Rechner angeschlossenen Chipkartenleser die jeweiligen Transaktionen steuern. Die Verbindung mit einem Mobilfunknetz kann dabei auch über ein mit einem Datenanschluß-ausgerüstetes Mobilfunktelefon erfolgen – man siehe z. B. "PC Professionell", März 1994, Seiten 253–260 oder "Cash Flow", 2/95, Seiten 140, 141.

Mögliche Anwendungen in Verbindung mit einer Chipkarte sind z. B. Authentisierung, Erzeugung von digitalen Signaturen, Kredit-/Debitkartenanwendungen, elektronische Geldbörse.

Eine besonders hohe Sicherheit kann durch asymmetrische kryptographische Verfahren erreicht werden, bei denen der private Schlüssel in der Chipkarte nicht auslesbar gespeichert ist und entsprechende Krypto-Verfahren in der Chipkarte nicht manipulierbar durchgeführt werden. Chipkarten-Bausteine für derartige Anwendungen sind heute auf dem Markt verfügbar, z. B. der Baustein SLE 44CR80S der Siemens AG.

Aufgabe der Erfindung ist es, den Anwendungsbereich des Mobilfunktelefons so zu erweitern, daß in Verbindung mit einem Rechner gesicherte Transaktionen in den ansteuerbaren Netzen möglich sind.

Dieses wird einerseits gemäß Anspruch 1 dadurch erreicht, daß das Mobilfunktelefon in der Weise erweitert wird, daß es zusätzlich als Kartenterminal für einen Rechner verwendbar ist, indem die Kontaktiereinheit über eine Steuereinheit mit der Anschlußschnittstelle für den Rechner koppelbar ist. An diese Steuereinheit können auch die übrigen für den Mobilfunkverkehr benötigten Bauteile angeschlossen sein, um weitere Steuerfunktionen zu ermöglichen.

Weiterhin ermöglicht die Verwendung eines solchen erweiterten Mobilfunktelefons gemäß Anspruch 3 in Verbindung mit einem Rechner, der unabhängig vom Funkteil des Mobilfunktelefons an ein Kommunikationsnetzwerk in bekannter Weise angeschlossen ist, daß ein Mobilfunktelefon-Inhaber ortsunabhängig von jedem beliebigen Standard-Rechner aus persönliche oder öffentliche Netzdienste, z. B. über das Internet, in Anspruch nehmen kann, die an die Sicherheit hohe Anforderungen stellen, ohne daß diese Standardgeräte über Chipkarten-Leseeinrichtungen verfügen müssen.

Weiterbildungen der Erfindung beziehen sich auf Verfahren zum Betreiben einer derartigen Gerätekombination. Diese betreffen u. a. das Betriebsbereitschalten des Mobilfunktelefons als Kartenterminal, das neben der Abwicklung von Netzdiensten in der üblichen Weise auch Verschlüsselungen bzw. Entschlüsselungen in an sich bekannter Weise ermöglicht.

Besondere Vorteile ergeben sich daraus, daß hochsensible Daten, wie z. B. die persönliche Geheimzahl PIN oder Geldbeträge am Mobiltelefon mit der Tastatur eingegeben und unverschlüsselt angezeigt werden können, bevor sie verschlüsselt an den Rechner weitergeleitet werden. Damit werden Eingaben über die Rechnertastatur vermieden, so daß Viren im Rechner die Eingaben nicht verfälschen können.

Auch besteht in vorteilhafter Weise die Möglichkeit, Kontrollwörter über das Mikrofon als Berechtigungsnachweis einzugeben, die dann digitalisiert an eine Kontrollinstanz im Kommunikationsnetz weitergeleitet und mit einem Referenzmuster verglichen werden. Auf diese Weise kann die Identität eines Benutzers zusätzlich anhand eines persönlichen biometrischen Merkmals verifiziert werden, was erhöhten Sicherungsanforderungen gerecht wird.

Weiterhin können auch Daten und/oder Steuerinformationen vom Rechner über die Anschlußschnittstelle an den Speicher im Mobilfunktelefon übertragen und dort abgespeichert werden. Damit ist es möglich, Daten auf der Chipkarte zu ändern oder zu speichern. Bei diesen Daten kann es sich z. B. um Schlüssel für die Verschlüsselung bzw. Entschlüsselung oder um einen Geldbetrag für eine Geldkarte handeln. Letztere eröffnet zudem die Möglichkeit eines Kartentelephons, indem beim Betrieb als Telefon ankommende Gebührenimpulse eine Abbuchung des jeweils entsprechenden Geldbetrages bewirken.

Einzelheiten der Erfindung seien nachfolgend anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert. Im einzelnen zeigen

Fig. 1 eine schematische Übersicht eines Rechners mit Netzkopplung und angeschlossenem Mobilfunktelefon als Kartenterminal für die Inanspruchnahme von Netzdiensten und

Fig. 2 eine schematische Darstellung einer Chipkarte für verschiedene Anwendungen.

Bei der Darstellung von Fig. 1 ist ein Mobilfunktelefon 10 über eine Standardschnittstelle 12, z. B. RS232, an einen Rechner 30 in Form eines üblichen PC angeschlossen. Die Schnittstelle 12 ist innerhalb des Mobilfunktelefons 10 mit einer Steuereinheit 11 verbunden, an die außerdem eine Kontaktiereinheit 13 für das SIM-Modul/die Chipkarte 14/14a, eine Anzeige 15, eine Tastatur 16, ein Sprach- und Funkmodul 17 sowie ein Speicher 18 angeschlossen ist. Das Sprach- und Funkmodul 17 hat dabei in üblicher Weise Zugang zum Mobilfunknetz 20.

Vom Rechner 30 sind lediglich die Anschlußschnittstelle 31 für das Mobilfunktelefon 10 mit dem zuständigen Treiber 32 gezeigt sowie ein sogenannter Browser 33 und Rechneranwendungen 34 für die Inanspruchnahme von Netzdiensten, beispielsweise im Internet, angedeutet, die über das Kommunikationsnetz 40 in Verbindung mit einem entsprechenden Anbieter 50, z. B. in Form eines sogenannten Servers, ausgeführt werden können.

Auf dem SIM-Modul oder der Chipkarte 14 bzw. 14a sind die mit Schlüssel zugänglichen Anwendungen gespeichert. Für die verschiedenen Anwendungen können individuelle Chipkarten vorgesehen werden. Es können aber auch, wie Fig. 2 zeigt, die Mobilfunk-Anwendungen für GSM/DCS 141 sowie die verschiedenen Internet-/Netzanwendungen 142, 143, 14x mit ihren unterschiedlichen Schlüsseln auf einer Chipkarte gespeichert sein.

Vor Nutzung eines der Netzdienste ist eine entsprechende Chipkarte auszuwählen und in die Kontaktiereinheit 13 des mit dem Rechner gekoppelten Mobilfunktelefons 10 einzusetzen. Außerdem ist der das Mobilfunktelefon 10 als Kartenterminal über die Anschlußschnittstelle 31 steuernde Treiber 32 mit der entsprechenden Treibersoftware zu laden.

Dies kann von einer Diskette aus erfolgen. Um jedoch Manipulationen am Treiber 32 auszuschließen, ist es zweckmäßig, daß die z. B. mit einem privaten Schlüssel des Mobilfunknetz-Betreibers signierte Treibersoftware von einem entsprechenden Server auf Anforderung vom Rechner 30 aus über das Kommunikationsnetz 40 in den Treiber 32 geladen wird. Danach kann dann automatisch eine Verifikation der Treibersoftware anhand eines entsprechenden und sich auf der Chipkarte 14/14a in einem Anwendungsbereich, z. B. 14x, befindlichen öffentlichen Schlüssel des Mobilfunknetz-Betreibers durchgeführt werden.

Die Treibersoftware arbeitet zweckmäßig entsprechend einem bereits festgelegten Standard, wie z. B. ISO 7816-3 und der von der PC/SC-Workgroup gemeinsam mit Microsoft festgelegten ICC Spezifikation (<http://www.smartcard-sys.com>)

Die Netzanwendung kann im Rechner 30, beispielsweise durch Aufrufen des Browsers 33 und Eingabe eines sogenannten "uniform resource locator" URL gestartet werden. Damit wird über das Netz 40 eine Verbindung zum Dienstanbieter 50 aufgebaut, und es können die gewünschten Dienste 51, 52, ... 5x in Anspruch genommen werden. Das angeschlossene Mobilfunktelefon 10 bzw. die Steuereinheit 11 verhält sich dabei wie ein übliches Kartenterminal. Abhängig von den vom Dienstanbieter 50 bereitgestellten Diensten 51, 52, ... 5x sind Chipkartenanwendungen 142, 143, ... 14x auswählbar und ausführbar, z. B. für die gegenseitige Client-Server-Authentisierung, für die Verifikation von Zugriffsrechten, für die digitale Signatur sensibler Daten, für die Erzeugung von Schlüsseln zur Verschlüsselung von Daten, für den Beweis eines Bestellvorganges, für die Bezahlung aus einer elektronischen Börse.

Gegenüber einem herkömmlichen Chipkartenleser ermöglicht die Erfindung zusätzliche Funktionen des Mobilfunktelefons, die eine erheblich höhere Sicherheit gewährleisten:

Am Internet angeschlossene Rechner sind prinzipiell aus dem Internet eingeschleusten Viren ausgesetzt. So kann z. B. ein Kontoüberweisungsbetrag, der über die Rechnertastatur eingegeben wird, durch einen solchen Virus verfälscht werden, bevor die Transaktion mit dem Internetserver korrekt abgeschlossen ist.

Mit einem Mobilfunktelefon als Kartenterminal kann diese Manipulation dadurch verhindert werden, daß von der Rechner-/Server-Anwendung veranlaßt wird, sensible Daten, wie z. B. Überweisungsbeträge, über die Tastatur 16 des Mobilfunktelefons 10 einzugeben. Der Steuereinheit 11 wird dies über einen Code mitgeteilt, wodurch die eingegebenen Daten einerseits an der Anzeige 15 unverschlüsselt wahrgenommen und überprüft werden können. Andererseits werden diese Daten durch eine Chipkartenanwendung 14x verschlüsselt oder signiert und an den Rechner 30 bzw. den zuständigen Server zur weiteren Verarbeitung übergeben.

In gleicher Weise kann bei Eingabe einer persönlichen Geheimzahl PIN, welche durch eine Rechner-/Netz-Anwendung angefordert wurde, die an der Tastatur 16 eingegebene PIN in der Chipkarte verschlüsselt werden, bevor sie an die Rechner-/Netz-Anwendung weitergeleitet wird.

Anwendungen mit höchsten Sicherheitsanforderungen erfordern oftmals eine Authentisierung auf Basis biometrischer Merkmale. Mit der hier dargestellten Erfindung läßt sich dies folgendermaßen realisieren:

Eine Anwendung 5x fordert nach erfolgreicher gegenseitiger Client-Server-Authentisierung auf Basis asymmetrischer Krypto-Verfahren den Benutzer als sogenannten Client auf, eine Sprechprobe abzugeben, z. B. ein vereinbartes Kennwort dreimal hintereinander in das Mikrofon 17 des Mobilfunktelefons 10 zu sprechen. Die Steuereinheit 11 lei-

tet dann, beispielsweise veranlaßt durch einen von der Anwendung 5x bzw. vom Browser 33 übertragenen Steuercode, den digitalisierten Sprachstrom in Form eines Bitstrings an die zuständige Anwendung, z. B. 5x, weiter. Diese extrahiert aus dem empfangenen Bitstring die persönlichen Sprachmerkmale und vergleicht diese mit z. B. auf Platten gespeichert 60 abgelegten Referenzmustern 6x, um die Identität des Benutzers anhand seiner Sprechproben zu verifizieren.

Die Erfindung schließt auch ein, daß im Rahmen einer Rechneranwendung 34 von einem Internet-Server in den Rechner 30 geladene Daten, wie z. B. Telefonlisten, Adressenlisten, Umsatzdaten, Preislisten, in den Speicher 18 des Mobilfunktelefons 10 geladen und auf der Anzeige 15 dargestellt werden können, wobei durch die Tastatur 16 eine Auswahl möglich ist.

Bei einer weiteren Rechneranwendung 34 können am Mobilfunktelefon 10 eingetastete oder eingesprochene, digitalisierte Daten in den Rechner 30 übertragen und dort oder in einem Netzserver weiterverarbeitet bzw. später oder von anderen Personen abgerufen werden.

Weiterhin ist es möglich, daß – angestoßen durch eine Rechneranwendung 34 – über die Anschluschnittstelle 31/12 in den Speicher 18 des Mobilfunktelefons 10 Programme geladen werden können, die in der Steuereinheit 11 zeitlich entkoppelt zum Ablauf gebracht werden können.

Schließlich können auch Anwendungen/Schlüssel – angestoßen durch eine Rechneranwendung 34 – auf der Chipkarte selbst geändert, gelöscht oder geladen werden.

In allen Fällen kann die Übertragung von Daten, Programmen oder Anwendungen zwischen dem Mobilfunktelefon 10 bzw. der Chipkarte 14/14a und dem Rechner 30 bzw. dem Netzserver integritätsgesichert oder verschlüsselt erfolgen. Die hierfür notwendigen Schlüssel sind entweder auf der Chipkarte bereits gespeichert oder werden vorher zwischen Rechner-/Netzserver-Anwendung und Chipkarte z. B. nach dem Diffie-Hellman-Verfahren ausgetauscht. Darüber hinaus kann das Mobilfunktelefon 10 ganz allgemein in analoger Weise für die Verschlüsselung bzw. Entschlüsselung von Daten verwendet werden.

Eine weitere Ausprägung der Erfindung besteht in der gemeinsamen Nutzung einer Chipkartenanwendung in GSM- und Festnetzen. Ein Beispiel hierfür ist die elektronische Geldbörse. Sie kann z. B. als Anwendung 14x auf der im Mobilfunktelefon 10 eingelegten Chipkarte 14/14a über eine Rechner-/Netz-Anwendung 33/34/5x aufgeladen werden und später während eines GSM-Telefongesprächs, z. B. durch einen von der Funkvermittlungszentrale gesendeten Impuls in regelmäßigen Zeitabständen – entsprechend den entfernungsabhängigen Tarifen – dekrementiert werden. Derartiges "vorausbezahltes" Telefonieren reduziert das Betrugsrisiko, dem Mobilfunkbetreiber heute vielfach ausgesetzt sind, erheblich.

Patentansprüche

1. Mobilfunktelefon (10) mit Kontaktiereinheit (13) für eine Chipkarte (14, 14a) als Berechtigungsnachweis für den Mobilfunkverkehr und einer Anschluschnittstelle (12) für einen Rechner (30), **dadurch gekennzeichnet**, daß die Kontaktiereinheit (13) über eine Steuereinheit (11) auch mit der Anschluschnittstelle (12) für den Rechner (30) gekoppelt ist und Daten zwischen einer Chipkarte (14, 14a) und der Anschluschnittstelle (12) über die Steuereinheit (11) austauschbar sind.

2. Mobilfunktelefon nach Anspruch 1, **dadurch gekennzeichnet**, daß mit der Steuereinheit (11) auch die

- anderen für den Mobilfunkverkehr vorhandenen Bauteile verbunden sind, so daß Eingaben über die Tastatur (16) oder das Mikrofon speicherbar und über die Anschlußschnittstelle (12) weiterleitbar sind bzw. über die Anschlußschnittstelle (12) ankommende Daten speicherbar und/oder auf der Anzeige (15) anzeigbar sind, wobei die anzuzeigenden Daten durch die Tastatur (16) auswählbar sind. 5
3. Mobilfunktelefon (10) nach Anspruch 1 oder 2 mit angekoppeltem Rechner (30), dadurch gekennzeichnet, daß der Rechner (30) unabhängig vom Mobilfunktelefon (10) an ein Kommunikationsnetz (40) angeschlossen ist und daß das Mobilfunktelefon (10) als angeschlossenes Kartenterminal arbeitend für die Inanspruchnahme von Netzdiensten in dem Kommunikationsnetz (40) verwendbar ist. 10 15
4. Verfahren zum Betreiben einer aus Mobilfunktelefon (10) mit gekoppeltem Rechner (30) bestehenden Gerätekombination nach Anspruch 3, dadurch gekennzeichnet, daß vor Inanspruchnahme von ein Kartenterminal erfordernden Netzdiensten zunächst der die Anschlußschnittstelle (31) für das Mobilfunktelefon (10) steuernde Treiber (32) mit der benötigten Treibersoftware geladen wird. 20
5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die Treibersoftware über das Kommunikationsnetz (40) von einem Server des Mobilfunknetz-Betreibers auf Anforderung in den Treiber (32) des Rechners (30) geladen wird und daß anhand der Signierung der Treibersoftware mit einem privaten Schlüssel in Verbindung mit dem zugehörigen öffentlichen Schlüssel auf der Chipkarte (14/14a) das Vorliegen der berechtigten Treibersoftware automatisch überprüft wird. 25 30
6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß nach Aufbau einer Verbindung vom Rechner (30) aus über das Kommunikationsnetz (40) zu einem Dienstanbieter (50) in Verbindung mit dem Mobilfunktelefon (10) als Kartenterminal Chipkartenanwendungen auswählbar und ausführbar sind. 35
7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß das Mobilfunktelefon (10) als Kartenterminal des Rechners (30) zur Verschlüsselung von sensiblen Daten verwendet wird. 40
8. Verfahren nach Anspruch 6 und 7, dadurch gekennzeichnet, daß im Rahmen einer laufenden Anwendung benötigte hochsensible Daten wie persönliche Geheimzahl (PIN) oder Geldbeträge über die Tastatur (16) des Mobilfunktelefons (10) eingegeben und von der Steuereinheit (11) in Verbindung mit der Chipkarte (14, 14a) verschlüsselt weitergeleitet werden. 45 50
9. Verfahren nach Anspruch 6 oder 7, dadurch gekennzeichnet, daß als Berechtigungsnachweis oder zur Kontrolle auch über das Mikrofon eingegebene Kontrollwörter an die Kontrollinstanz der eröffneten Anwendung weitergeleitet werden, so daß in Verbindung mit hinterlegten Referenzmustern eine Verifizierung des Benutzers durchführbar ist. 55
10. Verfahren nach einem der Ansprüche 6 bis 9, dadurch gekennzeichnet, daß im Rahmen einer Anwendung vom Rechner (30) übernommene Daten an den Speicher (18) des Mobilfunktelefons (10) weitergeleitet werden. 60
11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß die vom Rechner (30) übertragenen Daten zur Änderung der Daten in einem Chip der Chipkarte (14, 14a) dienen. 65
12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß bei einer als Geldkarte dienenden Chip-

karte (14, 14a) die während einer Funkverbindung des Mobilfunktelefons (10) eintreffenden Gebührenimpulse eine Abbuchung des entsprechenden Geldbetrages bewirken.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

FIG 1

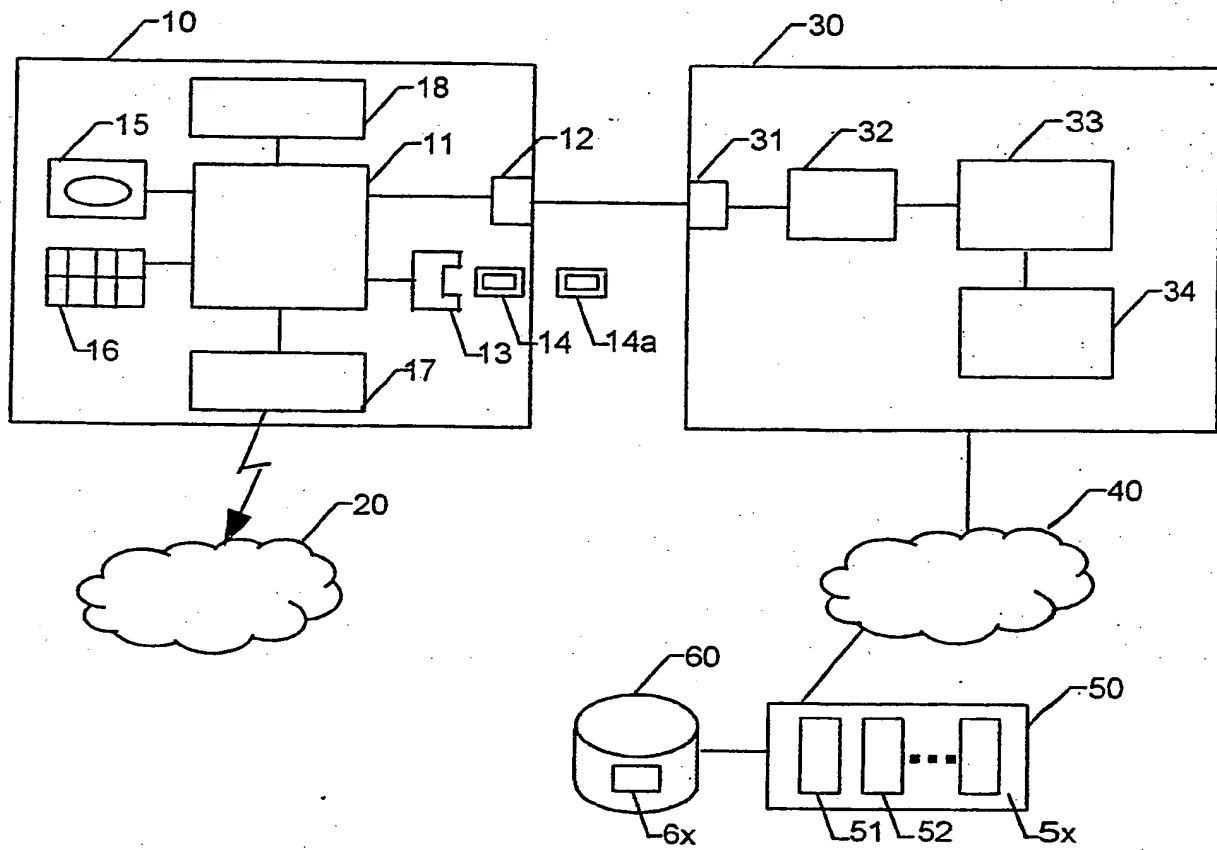


FIG 2

